	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 1 of 40

KSC PCGOAL System Data Integrity Position Paper

June 16, 2006



	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 2 of 40

Table of Contents

1.0	Evaluation Team Members	3
2.0	Assessment / Evaluation Approach	3
3.0	Risk Assessment	4
4.0	Data Reviewed	5
5.0	Findings, Observations, and Recommendations	10
5.1	Priority Metrics	10
5.2	Data Integrity Study Conclusions	11
6.0	Recommendation	28
7.0	Minority Report (dissenting opinions)	28
8.0	Lessons Learned	29
8.1	Customer Expectations	29
8.2	Terminology	29
8.3	Requirements	29
8.4	Programmatic Processes	30
9.0	References	31
10.0	List of Acronyms	32
	Appendix A Findings and Recommendations Prioritization Metrics Approach	36
	Appendix B Prioritization Worksheet	40

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 3 of 40

NESC Position Paper


ITA #: 04-035-E	
Requestor Name: Melanie Mulligan NASA Kennedy Space Center	Requestor Contact Info: (321)-861-4114 Melanie.J.Mulligan@nasa.gov
Short Title: KSC PCGOAL System Data Integrity	
Description: Request independent assessment of methodology used to arrive at probability of data corruption in the KSC PCGOAL computer systems.	
Date Received: March 31, 2004	Date ITA/I Initiated: April 20, 2004
NESC Chief Engineer (NCE) Assigned: Tim R. Wilson	NCE Contact Info: (321) 861-3868
Leads Assigned: Robert A. Kichak Steven S. Scott	Lead Contact Info: (301) 286-1199 (301) 286-2529
Date ITA/I Concluded: July 8, 2004	

1.0 Evaluation Team Members

Robert A. Kichak, Co-Lead, NESC Discipline Expert for Power & Avionics
Steven S. Scott, Co-Lead, NESC Discipline Expert for Software
Thomas G Bialas, GSFC
Walter B. Thomas, GSFC
Michael B. Uffer, Honeywell HTSI
Kevin L. Hames, JSC
Kevin S. Tones, JSC
Navid Dehghani, JPL
Allen Terry Morris, LaRC
Sally T. Yamashita, Aerospace Corp.
Sophia A. Chow, Aerospace Corp.
Lorena C. Vajda, Booz Allen Hamilton
Nelson E. Barry, Booz Allen Hamilton
Ken Costello, NASA IV&V
Deborah Kromis, NASA IV&V
Robert F. Hodson, LaRC (written review & comments)

2.0 Assessment/Evaluation Approach

System Assurance Analyses (SAAs) have been conducted on several critical Kennedy Space center (KSC) computer systems. The potential for data corruption inherent in these systems

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 4 of 40

drives a large number of Critical Item List (CILs) with resultant operational constraints. An SAA conducted for upgrade of the KSC engineering advisory tool PCGOAL from a DOS to Windows platform highlighted 195 data corruption CILs. PCGOAL is assessed as “critical” because it is used to buy test requirements, make launch commit criteria violation calls, and support real-time decisions during hazardous testing. The KSC engineering community has developed a method for assessing these data corruption CILs to determine the probability of failure. The results of this assessment may be used to eliminate the CILs entirely by classifying the failures as “not credible.” KSC Safety and Mission Assurance (S&MA) has requested an independent technical assessment of the methodology employed to assess and retire the PCGOAL data corruption CILs. Resolution of this issue has potential to impact numerous SAAs, not only for this system but all others classified “critical” since the methodology used to eliminate these data corruption CILs can be employed elsewhere.

NESC involvement was initiated by KSC S&MA who elevated this problem for NASA Engineering and Safety Center (NESC) attention due to its complexity and the potential impact to the design and operational employment of critical command and control systems. The key concern is that the analysis approach requires independent assessment and validation.

The KSC NESC Center Chief Engineer, Mr. Tim R. Wilson, performed the initial risk assessment and presented the issue to the NESC Review Board (NRB) on April 1, 2004. Following the presentation, the NESC Deputy Director, Dr. Paul Munafo, assigned the NESC Discipline Expert for Power and Avionics, Mr. Robert A. Kichak, to research the issue and report back to the NRB.

3.0 Risk Assessment

The problem statement is potential for data corruption in complex computer systems drives a large number of CILs with resulting design and operational impacts. An analytical method for assessing and retiring these CILs has been developed and requires independent validation.


The results of the initial screening checklist were:

Checklist Item C

- Lack of technical consensus: Experts have conflicting opinions regarding the underlying assumptions and overall methodology used to arrive at data corruption failure probabilities.

Checklist Item H

- Issue involves Criticality 1 or 1R systems / components: PCGOAL advisory system is used to make launch-critical, real-time decisions.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 5 of 40

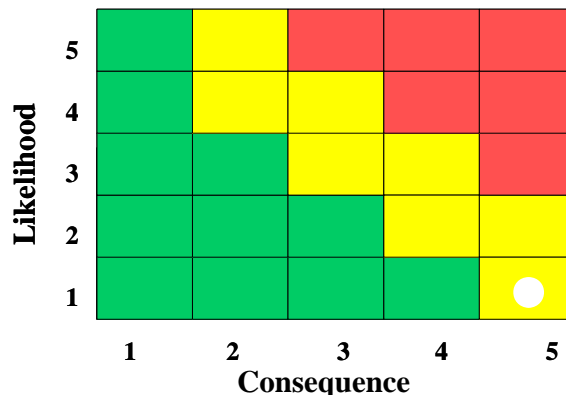
Checklist Item I

- Issue involves single-point failure exceptions or waivers and the approach taken to retire specific CILs.

The KSC PCGOAL Data Integrity initial Risk Assessment results are shown in the figure below.

KSC PC GOAL Data Integrity Initial Risk Assessment

L x C = 5




- Likelihood (1)
 - No instance of data corruption has been observed that has led to an incorrect conclusion or catastrophic event.
 - **Note: Determination of “likelihood” is the subject of this assessment**
- Consequence (5)
 - Potential loss of crew / flight vehicle due to incorrect decision made on the basis of corrupted data, or failure of command to effect desired response.

4.0 Data Reviewed

The NESC evaluation of KSC PCGOAL Data Integrity included both face-to-face meetings and teleconferences with the author of the study, Mr. Jeff Lee of United Space Alliance (USA) and several additional key USA and KSC personnel.

On Monday April 5th and on Friday April 9th, preliminary telecons occurred with Tim Wilson and others to discuss the Data Integrity Independent Test/Analysis Inspection (IT/AI) request and initial Center Chief Engineer Assessment that had been presented at the April 1, 2004 NESC Review Board. This was in response to Paul Munafo’s request that Robert Kichak review the issue presented by Tim Wilson and report back. The initial telecon on April 5th included the following attendees:


	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 6 of 40

Bob Kichak/NESC (Power & Avionics NDE)
 Tim Wilson/NESC (KSC NCE)
 Steve Scott/NESC (Software NDE)
 Jeff Lee/USA
 Wayne Morris/USA
 Larry Carr/USA
 Tim McKelvey/KSC
 Walt Thomas/GSFC (Reliability)
 Dave Bogard/GSFC (Reliability)
 Gloria Draus/KSC
 Martha Chu/GSFC (GSFC Information Systems Division)

Jeff Lee of USA presented the Data Integrity Issue scope and background to the attendees. He said that a white paper had been prepared, and agreed to provide it to the NESC for review. He expressed a desire to have another set of eyes review and assess the work done including the methodology, assumptions, findings, and recommendations. The white paper titled “Engineering Study Hypergolic Maintenance Facility (HMF) Hardware Interface Module (HIM) Card to Consumer Data Integrity Analysis KSC-5200-6561 Draft 10.0” is approximately 200 pages in scope and was assembled over the course of several months of effort. Rather than an independent data integrity analysis, an expert review of the existing analysis as described in the white paper was requested. It was stated that it is generally believed that this is not a heavy risk item, and the system has indeed proved itself to work very well historically. However, the criticality of the data is high. Three possibilities were the focus of the HMF Data Integrity concerns: 1) loss of data, 2) corrupted data that is recognized and 3) corrupted data that is not recognized. As described, various elements of computer hardware, software, Commercial-Off-The-Shelf (COTS), system architecture, and network interfaces are involved. Gloria Draus of KSC agreed to provide a link to detailed study information for the team to review. A second telecon was scheduled for Friday April 9th.

The second telecon on Friday April 9th included the following attendees:

Gloria Draus/KSC
 Tim Wilson/NESC (KSC NCE)
 Cynthia Null/NESC (Human Factors NDE)
 Kevin Hames/JSC (Power & Avionics SPRT)
 Glenn Williams/GRC (Power & Avionics SPRT)
 Walt Thomas/GSFC (Reliability)
 Tim McKelvey/KSC
 Jeff Lee/USA
 Larry Carr/USA

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 7 of 40

Kevin Hames noted that it appeared that the PCGOAL change had initially brought into question the validity of data, but that the scope now appeared much broader including possibly a wide range of network/workstation data retrieval and monitoring systems. Larry Carr said that critical items are indeed now tied to the KSC network infrastructure by the present SAA. The SAA on Data Impersonation |Corruption dove multiple CILs. The Program had requested a quantitative look at undetected errors and the risk of data corruption by network equipment. A simplified block diagram of the overall KSC Launch Processing System (LPS) Data Flow is shown in Figure 4.0-1.

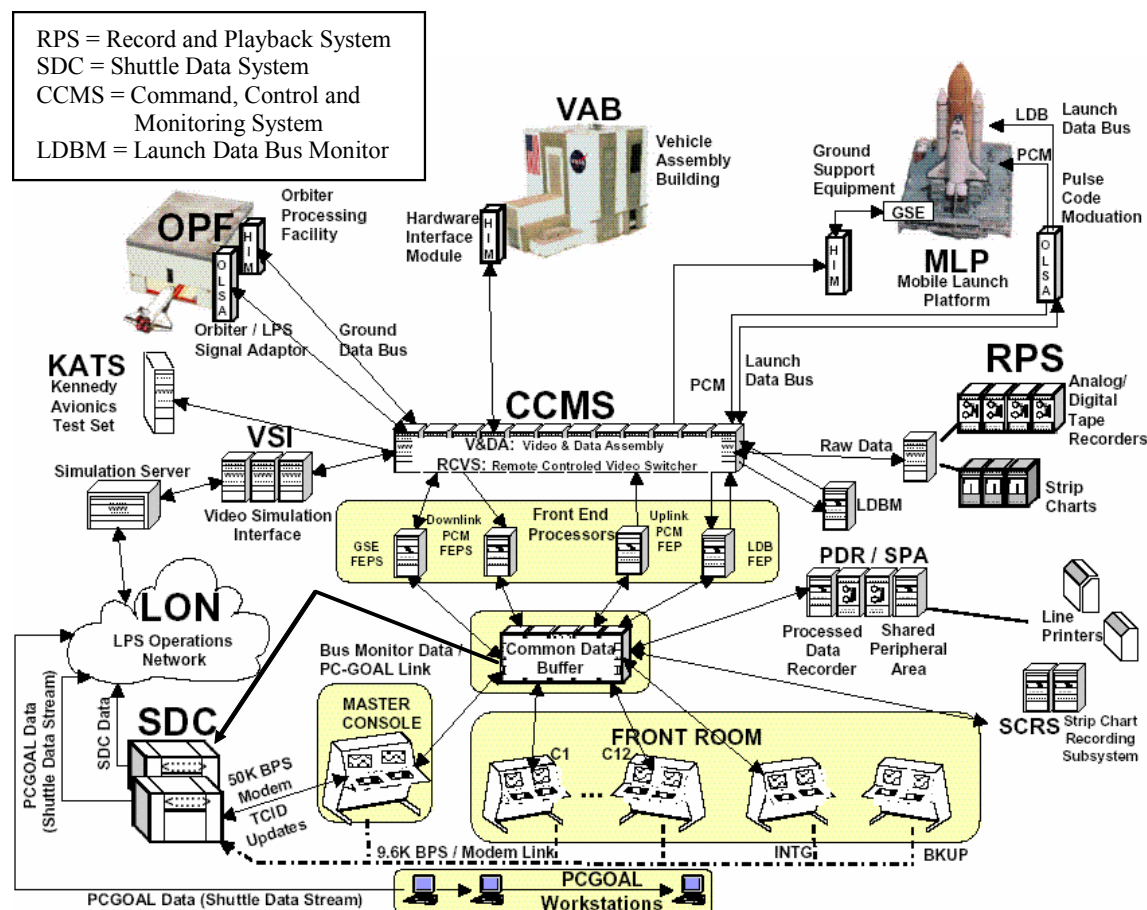



Figure 4.0-1. Simplified Block Diagram of the Overall KSC Launch Processing System (LPS) Data Flow

The PCGOAL system provides monitor-only data to control rooms and external customers. It also provides plot data for all configured measurements. A simplified sketch of the PCGOAL system is shown in Figure 4.0-2. PCGW is PCGOAL/Windows.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 8 of 40

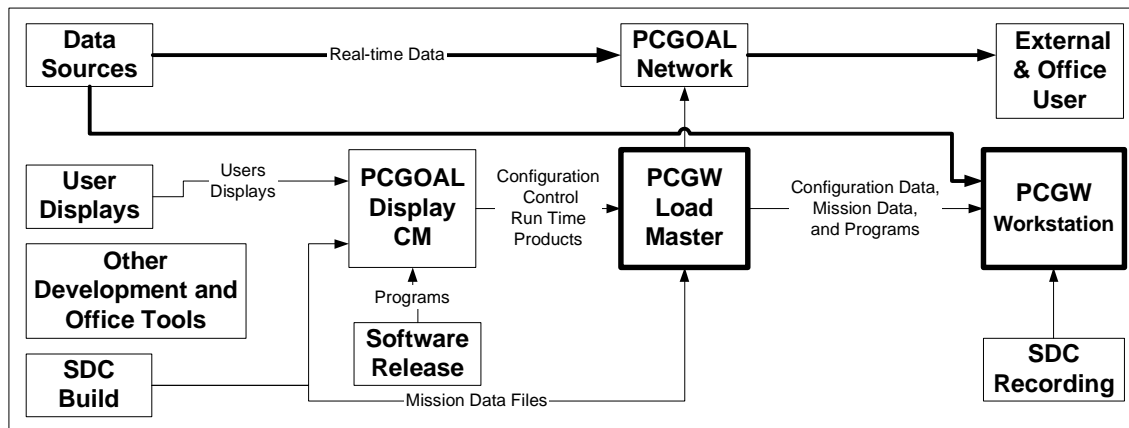



Figure 4.0-2. Simplified Sketch of the PCGOAL System

An Engineering Study and Data Path Analysis was performed by KSC, and this is what had been requested for review by the NESC. The HMF has all the data paths, and served as a good model for the data path analysis. A major question is whether the network, including hardware and software elements, should or should not be considered a critical item. The analysis studies each data path element, possible error modes, mitigations in place, and likelihood. It was also noted that critical measurements typically involve multiple sensors and data points.

Based on the telecon and subsequent discussions between Robert Kichak and Steve Scott, the co-chairs recommended that this request be handled as an NESC Consultation rather than as an IT/AI in an email that was sent from Robert Kichak to the NESC Director on April 19, 2004. The rationale is that an independent analysis has not been requested, but rather a review of an existing analysis. Also, it was noted that actual symptoms of unexplained data path integrity issues had not been manifested during the history of operations. The planned response was for a face-to-face consultation/review of two days duration at KSC with appropriate NESC-provided experts. The requestor's stated desire was for the NESC to identify the appropriate key individuals and arrange for the review before the end of April. Based on near term schedules, April 26th and 27th at KSC was targeted as ideal. The consultation was co-chaired by Bob Kichak and Steve Scott since both hardware and software elements were involved. Dr. Cynthia Null had suggested that it is most important that someone with a statistical background also be a part of the review. Walt Thomas of the GSFC Reliability Office agreed to fulfill that role. The KSC PCGOAL Data Integrity Consultation was approved at the NESC Review Board on April 20, 2004. Steve Scott and Robert Kichak were designated co-chairs for the review and the formal Review Team was established as previously described which included experts from GSFC, JPL, JSC, GRC, and LaRC, Booz Allen Hamilton, and The Aerospace Corporation.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 9 of 40

At the overview session on April 26, 2004, at KSC, Jeff Lee described the primary purpose, as shown in Figure 4.0-3.

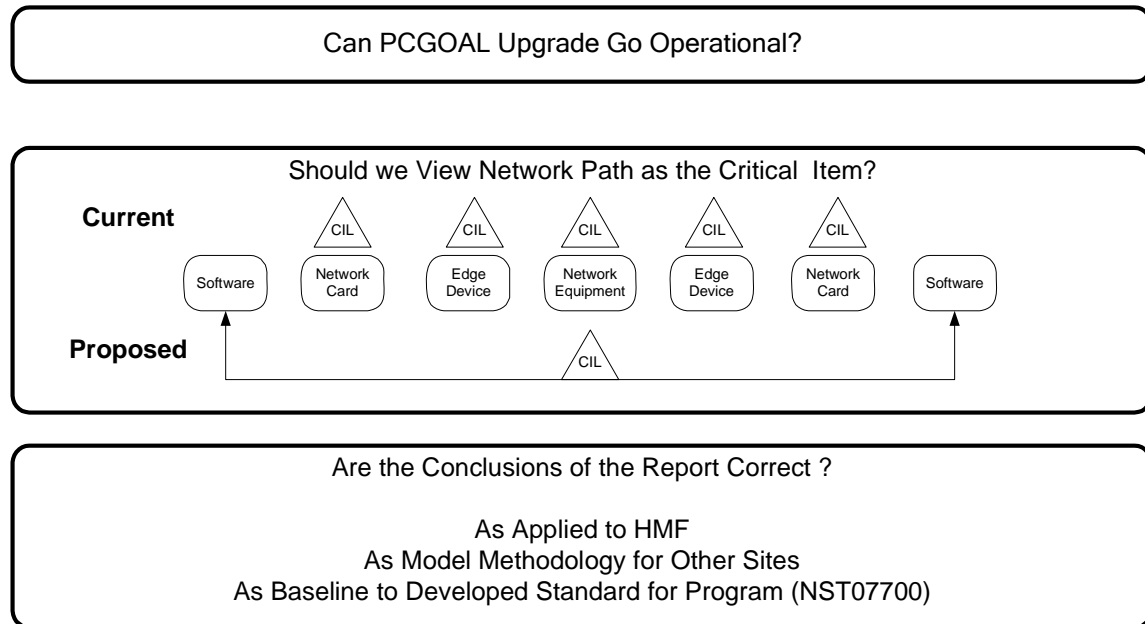



Figure 4.0-3. Overview of PCGOAL

The following were identified by Jeff Lee as some items appropriate for the Team's evaluation:

- Methodology
- System Representation
- Failure Mode
- Mitigations
- Model Structure
- Math Suitable and Accurate for Problem?
- Driving Parameters
- Resulting Number
- Clarity of Report

The Team was also requested to assess the seven conclusions of the study and to state whether we concur, do not concur, or have no finding and/or leave evaluation for KSC.

The Team specifically reviewed two major components of the system: PCGOAL which is a monitor and display system, and components and links that comprise the end-to-end downlink system.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 10 of 40


The draft report of analysis of the components and links (network) in the end-to-end downlink system “Engineering Study HMF HIM Card to Consumer Data Integrity Analysis KSC-5200-6561 Draft 10.0” as previously identified was distributed to the Team and was the basis of most of the questions, answers, and evaluation. A major issue was the large number (over 400) CILs that are open on the integrity and performance of various components of the end-to-end data system. It was stated during the review that due to time constraints and lack of sufficient staffing, closing all the 400 CILs individually was not possible. There was a lengthy discussion on the validity of the CIL process for this application since most of the components were COTS and unless each equipment component were replaced with a “better version” nothing could be done to address the CIL. Another major issue in this area is the apparent lack of an overall system performance and reliability requirement. Without requirements it is impossible to evaluate the performance and reliability of the system. The Team was presented with the performance numbers that the system is capable of, and no basis for judging if this was good enough. It was also not clear to the Team who or what level of organization is the owner or is responsible and/or accountable for this end-to-end network or data path system.

The PCGOAL system has been ported from a DOS-based system (486 processor) to a Windows-based system (basis for renaming it to PCGW). The porting has been completed (as of March 1, 2004). Although PCGOAL is not in the command and control loop, it is still considered a critical system for the return of the Shuttle to flight status because the information provided by the system is used to make critical decisions that could affect loss of life/loss of vehicle. While the porting itself seemed straightforward, there was no supporting documentation for this activity because the system had already gone through an Operations Readiness Review (ORR). However, a report from the ORR along with final test results would have helped the Team better access the completion of this task and its compliance with requirements.

5.0 Findings, Observations, and Recommendations

5.1 Priority Metrics

Approximately 50 findings were identified as a result of NESC review team’s evaluation of the data integrity and validation study “Engineering Study HMF HIM to Consumer Data Integrity Analysis - KSC 5200-6561.” To organize and prioritize these findings in a manner that minimizes impact and inadvertent change to the study’s content and merits, weighted metrics were established and applied to each finding to prioritize recommended changes. Factors for Criticality of Implementation, Viability to Implement, and Level of Effort versus Benefit were defined and assigned numerical scores by the Team. An Implementation Indicator was also

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 11 of 40

defined and numerically derived from these factors, resulting in a Recommended Implementation Priority. The specific approach and results are described in detail in Appendix A of this report.

5.2 Data Integrity Study Conclusions


The Findings, Observations, and Recommendations are sequentially numbered to aid discussion. Note that these recommendations do not require formal Program response. The Team considers the following Findings and Recommendations to be our top ten: 2.5, 2.7, 3.1, 3.2, 3.7, 3.8, 3.9, 4.6, 4.7, and 4.10. These Findings and Recommendations generally address two major themes: 1) a need for Independent Validation and Verification (IV&V) of PCGOAL, and 2) a need to define how reliable the network and data must be with assurance that data packets remain unmodified or disclosed during transmission, and then measure, track and evaluate metrics to show that the network meets these numbers to be able to address the CIL issue. Findings and Recommendations 4.12, 4.16, 4.17, 4.18, 4.19, 4.22, and 4.24 also scored highly in our assessment and address the technical merits, approach, and performance metrics of the methodology. The essence of these findings is on the validity of USA Inc.'s methodology. These issues are addressed by Finding 3.9 and are therefore redundant. An independent assessment of USA's methodology will reveal and address all of these seven findings both quantitatively as well as qualitatively. Finding 4.9, although highly scored by the Team, may be outside the scope of the assessment. Finding 4.21 is covered via monitoring, loading and identification of network errors as addressed in Finding 3.7 and is redundant. Findings 3.4, 3.5, and 3.6 are observations related to the JSC Mission and Launch Control Centers rather than the KSC LPS, and therefore are being referred to the NESC Chief Engineer at JSC.

5.2.1 Responses to Specific Customer Questions

The customer requested that the NESC Review Team consider seven specific conclusions of their Data Integrity Study, and comment on these as well as state whether we agree, disagree, or defer judgment to KSC as follows:

1.1 “The method and analysis in the Engineer Study HMF HIMs to Consumer Data Integrity KSC-5200-6561 are consistent with good engineering practices”.

Finding 1.1. The Team was in general agreement with this statement. However, the Team also noted some areas of deficiency in the analysis that need improvement. These are identified in Section 4.0 “Specific Recommended Improvements for the Data Integrity Analysis and Report”. In general, the continuously monitored and proven reliable HMF network, along with redundancy and fault tolerance, mitigate concerns about data loss.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 12 of 40

Recommendation 1.1. Incorporate the specific recommended improvements for the Data Integrity Analysis and Report contained in Section 4.0.

1.2 “Engineer Study HMF HIMs to Consumer Data Integrity KSC-5200-6561” presents an accurate depiction of the data paths under review.

		End to End		This Segment		End to End	
End To End Path	Loss Of Data Run Days	Undetected		Undetected		Undetected	
		End To End Run Years	Loss Of Data Run Days	End To End RunYears	Loss Of Data Ops Days	End To End Ops Years	Loss Of Data Ops Days
CCMS to Local Display	31.6	82.7	31.6	82.7	66.5	173.6	66.5
CCMS to Recorder	15.0	60.4	28.7	224.4	31.6	126.9	31.6
CCMS to Retrieval	15.0	41.3	16959.0	130.1	31.6	86.6	31.6
CCMS to PCGOAL	0.0	49.7	0.0	124.8	0.1	104.4	0.1
CLCS to Local Display	34.7	115.7	34.7	115.7	72.9	243.0	72.9
CLCS to Recorder	34.7	80.9	46026.1	268.2	72.9	169.8	72.9
CLCS to Retrieval	34.6	49.9	16959.0	130.1	72.7	104.7	72.7
CLCS to PCGOAL	0.0	63.9	0.0	142.6	0.1	134.2	0.1

Finding 1.2. The Team is not sufficiently familiar with the KSC Data Processing System to be able to assess this statement and defers that judgment to KSC. The methodology used to arrive at the conclusions in the data tables was described, and comments in Section 4.0 also apply.


Recommendation 1.2 – KSC should continue to monitor the network. Metrics should include Operational Availability, Reliability, Mean Times Between Failures (MTBF), Mean Times to Repair, etc. These metrics should be reported to senior management on a regular, on-going basis. Levels should be determined that would trigger an investigation.

1.3 “Basic conclusion:

- No path indicated a undetected error rate that should be a concern
- Top contributors to lost or erroneous data
 - Acquisition of data – (input processing)
 - Display of data – (reading, processing and driving display)
- Transmission and processing path very good”

Finding 1.3. NESC personnel were informed that the data error rate in the network was very low. Written reports seem to confirm this, although it is not clear that all the data was presented and it appears that reliability estimates were based on qualitative rather quantitative methods. Top contributors to lost and erroneous data were identified. Data Integrity is measured and monitored.

Recommendation 1.3. The possibility of data getting corrupted but not being recognized by operators as bad data drove an exploration of PCGOAL and the suggestion by NESC personnel that the West Virginia IV&V Facility perform an evaluation of any major changes to the network

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 13 of 40

and its method of verification and validation as a normal course of doing business. NESC also suggests that Human Factors personnel review the Human Interface Design of PCGOAL to ensure that it complies with Industry and NASA standard Human Factors Design Guidelines and effectively communicates to users any symptoms of data corruption.

1.4 “No significant risks have been identified in this study. The risk of data corruption by network equipment is no greater than other factors when protection and detection features are provided at the system level”.


Finding 1.4. The terms “significant” and “other factors” are a problem for the Team in this statement since they are vague and qualitative rather than quantitative. No quantitative requirements for data integrity/reliability were presented.

Recommendations 1.4. The Project should continue and even enhance its network monitoring capabilities. Metrics for data integrity/reliability should be established. Network block diagrams and reliability estimates should be clear and quantitative. Operational Availability or system reliability below an established high level should be flagged for immediate investigation. Replacement units for network components should have identified reliability levels and should be certified to meet those levels before installation. The CIL process should be driven by architectural changes, not mere replacement of COTS equipment. The Failure Mode Effects and Criticality Analysis (FMECA) process should be used to evaluate major system architectural changes and to establish the need for failure tolerance and redundancy, not as a substitute for network trouble reports or problem reporting and corrective action.

1.5 “The SAA should be modified to analyze and confirm that the system design has protection and detection features to allow it to be operated with known error conditions in the transmission path”.

Finding 1.5. NESC personnel agree with this apparent recommendation to avoid the tedious CIL process for every individual network component. The configuration and reliability of the network should be well known. Fault Tolerance and redundancy should be well characterized. Schedules for routine replacement of network components should be established on a sound actuarial basis. Characterization of the network reliability should be quantitative.

Recommendation 1.5. The HMF network should use standard industry and government practices for high reliability networks. The Project should continue and even enhance its network monitoring capabilities. Metrics for data integrity/reliability should be established. Network block diagrams and reliability estimates should be clear and quantitative. Operational availability or system reliability below an established high level should be flagged for immediate investigation. Replacement units for network components should have identified reliability levels and should be certified to meet those levels before installation. The CIL process should be driven by architectural changes, not mere replacement of COTS equipment. The FMECA

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 14 of 40

process should be used to evaluate major system architectural changes and to establish the need for failure tolerance and redundancy, not as a substitute for network trouble reports or problem reporting and corrective action.

1.6 “SAA Process would result in the generation of a ground rule which would downgrade the failure mode of corruption of data for retrieval/data collection transmission paths and existing CILs would be eliminated”.


Finding 1.6. It is not clear that an acceptable way of identifying potential problems would still be in place if the CIL process were eliminated immediately. However, the operative CIL process seems to be a long-perpetuated misapplication of the FMECA to network problem reporting and corrective action. What is needed is a network trouble reporting system more compatible with industry and government standards rather than forcing the FMECA/CIL processes into providing a substitute system.

Recommendation 1.6. Before existing CILs could be eliminated, it must be demonstrated that a mechanism is in place to identify potentially critical failures and require their resolution.

1.7 “COTS Network Equipment should be removed from the CIL for purpose of data integrity”.

Finding 1.7. Provided the mechanisms for measuring, monitoring, and ensuring network reliability and operational availability noted above are in place, NESC agrees that specifically calling out COTS equipment is not the best approach and is a misapplication of the FMECA/CIL process.

Recommendation 1.7. It would be acceptable for the entire network path to be included as a single item on the Critical Items List for the purpose of data integrity without identifying individual components in accordance with the Project’s recommendation unless a problem were identified. For this purpose a network trouble reporting system or problem reporting and corrective action system should be used in place of the CIL process. Proactive component reliability certification and scheduled maintenance/replacement in accordance with an established Logistics Support Plan is recommended as well.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 15 of 40

5.2.2 Additional Findings and Recommendations regarding the CIL Process and Lack of Requirements

The Team identified nine Findings and Recommendations that are related to application of the CIL process to the Data System and to lack of requirements. These are detailed as follows:

Finding 2.1. The CIL/Waiver process is a misapplication to the network reliability/operational availability/data integrity issue and should be replaced with a more standard government/industry practice except when major architectural changes dictate a major change or re-performance of the FMECA.

Recommendation 2.1. Stop using the CIL/Waiver system for the network and simple replacement of COTS units. Use CILs only when major architectural changes dictate that the Failure Modes and Effects analysis be repeated. Use waivers only when requirements are not being met. Instead, establish minimum reliability requirements for like replaceable units, and testing or burn-in requirements for network components.


Finding 2.2. The lack of formal reliability and data integrity requirements are driving the KSC system to generate unnecessary and pointless CILs. The plethora of CILs on these systems diverts resources from real issues to these which seem to not be truly worthy of a CIL.

Recommendation 2.2. 1) Develop and provide to all of the control centers reliability and data integrity requirements against which the systems may be built; 2) Apply CILs only to truly credible failures. Revise the rules for creating CILs; and 3) Write waivers only when the aforementioned requirements are not met. Note: The reliability should be based on the state-of-the-art and the reasonable requirements of the Program. The requirements should also state clearly mitigation methods and which ones are considered effective mitigation techniques.

Finding 2.3. CIL process (and work-off and closure) appears to treat low probability small items (e.g. network devices) at the same level as something like the Common Data Buffer. This approach creates the possibility that a “bigger CIL” would be worked later or has less time for its work-off.

Recommendation 2.3. CILs should continue to be documented. Grouping of CILs should be completed and/or continued to facilitate and improve CIL work-off. Additional prioritization/categorization is needed to differentiate between items whose occurrence has a higher likelihood of resulting in human loss or other serious impact. As an example, if the C&C string goes down, the impact could be severe due to the length of the outage, whereas a bad telemetry point is unlikely to be used (by itself) and lead to a serious impact.

Finding 2.4. The current CIL process does not guarantee network performance. Component level performance does not guarantee overall performance.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 16 of 40

Recommendation 2.4. Set measurable network performance requirements:

- Latency
- Bit Error Rate (BER)
- Throughput
- Routing

Treat network as a system, not a list of components.

Finding 2.5. Without quantifiable requirements for KSC's Ground Support Equipment (GSE), everything should be done to ensure the integrity of this safety-critical system. Various relationships need to be investigated more thoroughly.

Recommendation 2.5. Investigate the following relationships more thoroughly:

- 1) MTBF and Undetected Errors (~1:1 relationship).
- 2) BER and loss of data.
- 3) The degree to which undetected errors and loss of data are influenced by overall network architectural structure or lower level driving parameters.


Finding 2.6. The Team was told that the CIL/Waiver approach requires box-level assessments. This is not appropriate for network systems, which require assessment at the system level since box-level compliance does not ensure adequate overall network performance.

Recommendation 2.6. The CIL/Waiver process needs to be investigated and perhaps replaced with another ground rule process that provides more quantifiable assurance to prevent catastrophic failure, particularly with the use of COTS hardware and software.

Finding 2.7. It is difficult to determine if a model or methodology is better or more acceptable without having some metric of comparison. There are no quantifiable requirements for data integrity.

Recommendation 2.7. There needs to be some quantifiable metric to determine if data integrity (end-to-end) is acceptable.

Finding 2.8. Validations Against Requirements – Requirement specifications (functional, technical, operational, and management) were not referenced. As a result, study conclusions and assumptions could not be validated. Page 198 of the study lists 13 specifications that are referenced as requirements, however the statements are ambiguous.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 17 of 40

Recommendation 2.8. Include or reference a ratified set of decomposed requirements (functional, technical, management and operational) in the study. If a Requirements Specification does not exist, it should be created, ratified and published.

Finding 2.9. Part of the mitigation of the impersonation issue is supported by the software at both ends of the data streams, specifically in terms of the PCGOAL data stream coming from the Shuttle Data Center (SDC). The current system seems rather robust not just in terms of the PCGOAL implementation but the other software used throughout the network. However, the changes to the PCGOAL program in particular may leave open some vulnerability as the architecture of the program is changed to move away from mostly custom written code to a COTS programming environment that includes vendor code that is not visible to the developers.

Recommendation 2.9. The PCGOAL2 project should be developed around clear and concise standards that include appropriate requirements and interface documentation and design guidance that supports the data integrity features implemented in the current version of PCGOAL. This should include identification of what the current data integrity features are and documentation of those features. Additionally, a risk assessment of the use of the COTS programming environment should be conducted to ensure that the environment is robust enough to support the development of a critical application with a high level of data integrity. This assessment should be documented so that any future changes to the program will have the appropriate background information to ensure that future data integrity remains intact.

5.2.3 Other Findings and Recommendations


The Team also identified 10 specific Findings and 13 Recommendations related to other aspects of the study methodology, assumptions, or conclusions. These are detailed as follows:

Finding 3.1. Regardless of network reliability and redundancy, the PCGOAL software could still incorrectly process or represent data.

Recommendation 3.1. The NASA IV&V Facility should perform an independent evaluation of the PCGOAL (to include PCGOAL2 and PCGOALW) software to gain additional assurance that this software meets its requirements, functions as intended, and accurately represents data to the user.

Finding 3.2. Incorrect, inadequate, or inappropriate representation of data to users could result in a poor decision by an operator. This may also apply to the Mission Control Center.

Recommendation 3.2. Perform a Human Factors study of the PCGOAL displays (PCGOALW and PCGOAL2 included) to determine if they are following NASA recommended and industry standard practice for representation of data, etc. Dr. Cynthia Null of NESC could lead/perform this study.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 18 of 40

Finding 3.3. The leased network from KSC to Dryden is treated as a black box even though systems more fully under our control are not. This is not only inconsistent it is wasteful of resources.

Recommendation 3.3. Treat networks, or sections of networks once designed and validated, as a black box and do not go down to the level of each box. Then allow the replacement of parts at the network so long as the design does not change without a full re-certification of all the boxes. Test the end-to-end network and so long as the requirements (numbers) are still met, let the network certification stand.

Finding 3.4. This review has surfaced many issues with the process of determining adequate reliability for a flight critical network. The review can be of use seemingly to all systems across NASA that support flight operations.


Recommendation 3.4. Perform a similar review for the Mission Control Center (MCC) at JSC as well as other flight support networks. It would seem the MCC review is a Return to Flight (RTF) issue since the KSC-Launch Control Center (LCC) review was also considered a RTF issue.

Finding 3.5. KSC seems to have a similar situation to that extant at JSC; that is there are two systems used in the LCC and MCC, respectively: one is a tightly configuration managed system that is certified for use and a second, less heavily configuration managed system that is used as heavily, if not more, than the formal system. In the MCC, the second system is the laptop next to each flight controller.

Recommendation 3.5. Review all of the assistive software not on the main MCC workstations that are used while on console. Although these are ostensibly not to be used to make calls, they are heavily relied on because they provide greater insight and understanding than the certified system. These applications and tools may well be necessary to operate the vehicle. The prohibition of the applications would seem unwise. The review should look at how such tools might be certified for use.

Finding 3.6. The issues and concerns addressed in this report at KSC begs the question why has this not been done for the MCC in Houston? The control center in Houston may not have gone to the level we saw here. Given the importance of the MCC it should be reviewed to this level. It is not clear that the MCC, built in the mid-1990s, was ever validated in this fashion.

Recommendation 3.6. The MCC in Houston should be validated in a similar fashion. The reliability of the network at MCC-JSC should be verified to be at least as good as the one at KSC.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 19 of 40

Finding 3.7. IP networks by design have error conditions. Error conditions can happen under normal conditions, but can be minimized by:

- Minimizing overall BER, and
- Minimizing network loading.

Recommendation 3.7. To minimize BER:

- *Monitor network for errors,*
- *Keep network loading well below network capacity, and*
- *Exercise great care when swapping in new equipment.*

Also, write/modify application code to detect “undetected” errors created by network – use application level CRC, encryption, compression, etc.

Finding 3.8. The actual numbers for the model were considered conservative by USA Inc. These numbers, however, were developed from experience and vendor-supplied data. Since one should not place much confidence in vendor-supplied data, actual numbers for the model should represent the worst-case conditions.


Recommendation 3.8. Use worst-case numbers instead of simple conservative numbers in the probabilistic model. Given that the Shuttle is a highly visible Program, everything should be done to ensure integrity within reason despite the lack of quantifiable requirements.

Finding 3.9. Though the methodology is acceptable, its conclusions should be independently validated both quantitatively and qualitatively.

Recommendation 3.9a. Use a different approach to compute the errors (and bounds on the errors) for the HMF HIM Card to Consumer Data Integrity Task. Compare this independent approach to USA’s methodology. If close, consider USA’s model as reasonably validated. This comparison should be quantitative as well as qualitatively based.

Proposal – Use USA’s methodology as one way of determining end-to-end data integrity. If the method is successfully and independently validated, it should be used as the baseline in the form of standard quantitative requirements. All other changes/modifications must meet or exceed the current quantified values.

Recommendation 3.9b. – It is assumed that archived/historical data on network performance over time exists, such as network and consumer errors or hardware failures or replacements versus system operating times. It would be prudent to begin “trending” these data. For an overall systems performance metric, plot cumulative network errors vs. cumulative network operating time(s) on a Crow-AMSAA (CA) plot. This is a log-log plot. They are well suited to

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 20 of 40


looking at system performance where multiple failure modes might exist and for which data may be incomplete or missing. The plot will show whether the system is operating statically, worsening or improving by the slope of the plotted data. Also, you may find breaks or cusps in the plot. These are related to system changes and are part of the analyses. If the plot shows a “stable” series of data (cumulative failures vs. cumulative time), then you can make predictions regarding future performance.

Recommendation 3.9c. Track hardware failures using Weibull plots to determine the character of the failures. This tool will indicate whether you’re experiencing infant mortal, random or wearout failures. Ideally, collect data on one type of component at a time, as the Weibull is best suited when one is dealing with only one failure mode. It can handle multiple failure modes, but analysis becomes more complex and requires more data. In tracking hardware failures using Weibull, you also must track and account for the operating times of the non-failed units. This is part of the analysis. If you do this (account for the non-failed unit hours) you will be able to predict future failures statistically. These data also will be useful for determining optimal replacement times for maintained components, to assure network availability.

Recommendation 3.9d. Caution: it was mentioned during the meeting that the network is required to be fully operational only during the pre-launch phase of your operations. Therefore, the tendency is to calculate a reliability, or Pf, using only this required operational or mission time – which is very short. However, in reality, your network is operated almost constantly. And any failure modes likely are “excited” during these normal operational activities. Therefore, using a “short required mission time” to determine network reliability/availability will produce incorrect or misleading results. Since the failure modes are continuously operative, you must use that time (continuous operating time) to compute and predict the system reliability. To calculate the “required reliability” during the short pre-launch time frame, use a conditional reliability calculation that accounts for the successful operation at the time prior to the pre-launch phase and predicts what will be the Ps during the following mission time.

Finding 3.10. During the meeting it was stated that PCGOAL is not in the launch commit criteria list (CCL). Additionally, the general sense of the meeting was that PCGOAL was not needed to process the Shuttles. It came across as a “nice to have”, although at the same time it was a “critical nice to have”.

Recommendation 3.10. While PCGOAL may not currently be in the launch CCL, the proposed change to the system may place it into that category. A detailed review of the use and integration of PCGOAL in the firing rooms should be conducted to re-evaluate whether a Shuttle launch could occur with the lack of PCGOAL. It is recommended the review should extend beyond to determine what impacts to Shuttle processing may occur by a loss of PCGOAL. Although there are few safety issues during Shuttle processing, it would seem prudent for the Shuttle Program to understand the impacts of a loss of PCGOAL and how that may affect launch schedules and costs.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 21 of 40

5.2.4 Specific Recommended Improvements for the Data Integrity Analysis and Report

Finally, the Team identified 24 specific recommended improvements for the study, detailed as follows:

Finding 4.1. The report structure is very difficult to follow, particularly for those not intimately familiar with KSC operations and processes.

Recommendation 4.1. An executive summary is needed, as well as an acronym list. Remove references to Checkout Launch and Control System (CLCS) if it is not relevant. Also recommend putting the bulk of sections 5, 7 and 8 in appendices and summarize their content in the main body of the report.

Finding 4.2. It is unclear what tools were used to provide data used in the analysis. The Team understands that PCGOAL software was one source, but other possible tools (e.g. network LAN analyzer, test sets) were not described. It was stated that HP Openview is used on the network, but unclear whether or not data gathered from Openview was used as input to this analysis.


Recommendation 4.2. Cite sources of data used in the report. Describe whether Openview data is used to validate the outcome of other sources of data, and how Openview is used in the user's environment.

Finding 4.3. Though sensitivity analysis was performed, the variables and guiding parameters that affect the model should be provided in a table showing upper and lower bounds and the effects of varying these parameters.

Recommendation 4.3. Include a table showing how all the variables and guiding parameters affect the model. Then, use the sensitivity analysis provided as a summary of the overall table. This table will help the readers to see the model's relationships and provide greater visibility in the final results.

Finding 4.4. The data integrity white paper describes a model based on a single string from input to consumers. Multiple instances should be investigated to increase the Program-wide probability of error.

Recommendation 4.4. Investigate multiple instances to determine a more realistic Program-wide probability of error. This investigation would be a study of maximum capacity to provide a bound on data integrity in worst case-conditions.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 22 of 40

Finding 4.5. The separability of system reliability from data integrity needs to be discussed more thoroughly. Although the verbal explanation was deemed sufficient, the discourse in the white paper was deficient.

Recommendation 4.5. There needs to be a discussion of the separability of reliability from integrity in the white paper. It needs to be transparent to the reviewer. Its inclusion would help to clarify the context of the model.

Finding 4.6. Approach/Methodology – The study did not reference the following essential methodologies:

- System Development Life Cycle (SDLC)
- Change Control
- Risk Management
- Assumptions


Recommendation 4.6. Document study Approaches/Methodologies to include sections in the document for Executive Summary, Assumptions, Risk Management, Life Cycle considerations, and Change Control.

Finding 4.7. Data Integrity Validation Requirements - The study did not satisfy its stated objective and requirement for data integrity. The following critical considerations required in a scientific study were not addressed, such as:

- Potential for human error.
- Error rate in data packet transmissions due to undetected errors, impersonation, software deficiencies, hardware malfunction, and catastrophic failure resulting from natural disaster.
- PKZip and MD5 are identified as the data compression and integrity algorithms. PKZip is strictly a compression algorithm and MD5 is strictly used for data confidentiality (versus integrity).
- Conversion, hashing, and encryption algorithms also were not referenced.

Recommendation 4.7. The requirements for data integrity assertions require that absolute assurance of end-to-end data packet reliability and accountability be established.

- *Employ the SHA1 compression and integrity algorithm specifically designed to address data integrity.*
- *Include a reasonable margin of error to compensate for human errors.*
- *Design and deploy a mechanism to identify and account for lost, spoofed, or impersonated data packets.*

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 23 of 40

- *Conduct an assessment of risk on the data integrity approach to identify residual risk, contingency plans and mitigation strategies.*

Finding 4.8. Dependencies - The study did not identify critical dependencies and thresholds that must be in place and operational:

- Environmental Considerations
- Power
- Cabling
- Timing

Recommendation 4.8. Document and include a section to identify “all” system dependencies and application, system and network interconnections.

Finding 4.9. Performance Baselines and Thresholds – Performance specifications and baselines were not identified in the study for uplink and downlink data streams, point-to-point network communications, points of failure, or software testing and evaluation benchmarking.

Recommendation 4.9. Establish and document performance metrics to establish baselines and thresholds for transmission rates, packet conversion, anomaly detection and dropped packet rates. Comprehensive reporting schedules and criteria should also be established.

Finding 4.10. Error Rate Assertions – Error rate assertions were not conclusive because several key data elements were not considered or included for consideration:


- Data sets supporting error rate assertions were not available or referenced.
- Lost data packets.
- Undetected errors.

Recommendation 4.10. Modify current error rate calculations to include lost packets, undetected errors, and existing data sets.

Finding 4.11. System Development Life Cycle Documentation was not cited or referenced in the study.

Recommendation 4.11. Reference specific System Development Life Cycle Documentation and milestone requirements to declare compliance. If this documentation does not exist, it is the Team’s recommendation the documentation be developed.

Finding 4.12. In review of Section 4.2, CCMS to Local Display and CLCS to Local Display data paths, there are concerns with the display interface module, specifically in the Hardware Interface Module (HIM) to the Ground Data Bus (GDB). The GSE coordinates polling HIM for

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 24 of 40

display data. The GDB transfers the data to the Front End Processor (FEP). FEP formats it according to standard protocols and displays the result to the monitor. The indication of a possible issue with data loss is when the polling mechanism can not keep up with amount of data available from the hardware interface module. Figure 5.2.4-1 (copied from the KSC-5200-6561) shows the HIM to FEP interface using GDB.

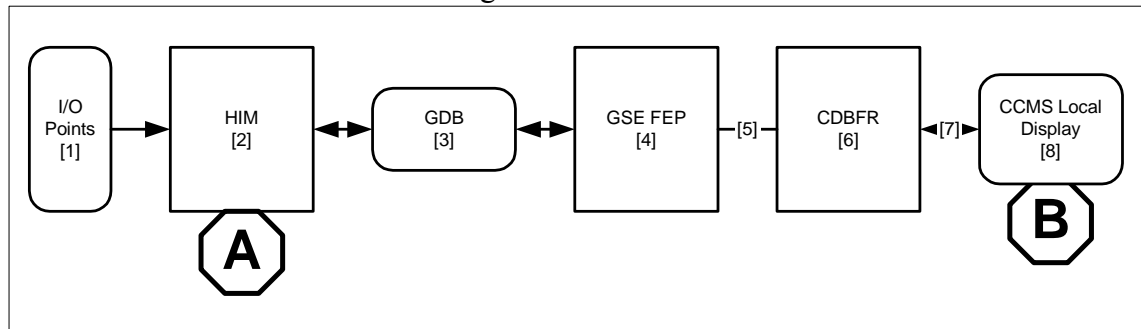


Figure 5.2.4-1. HIM to FEP Interface using GDB

Recommendation 4.12. To fully analyze this path (and perhaps discount it as a data loss path), the following questions must be answered:

1. *What is the average and maximum (burst) data rate in the hardware interface module?*
2. *Is there buffer provided in the hardware interface module? How Much?*
3. *What is the maximum latency of the data polling collection?*
4. *Is the polling mechanism timing deterministic?*

Finding 4.13. Section 5.3 (CCMS to Shuttle Data Center and PCGOAL), specifically pages 48-49 (Sections 5.3.2 & 5.3.2.1). Figure 5.2.4-2 (copied from the KSC-5200-6561 document) shows the specific elements of this data transfer.

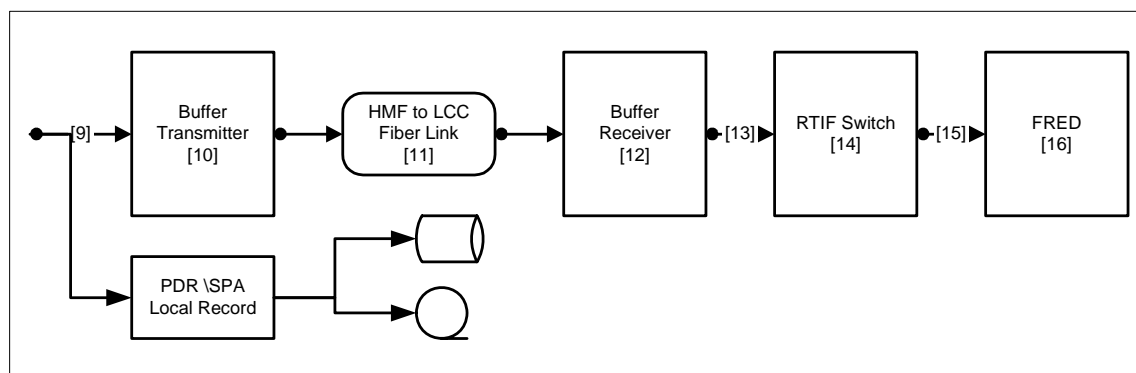



Figure 5.2.4-2. Specific Elements of Data Transfer

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 25 of 40

The buffer transmitter/receiver interface link functions by converting 16-bit parallel data to serial data, transmitting them over the fiber link interface and converting them back to 16-bit parallel data. Although this link has sufficient bandwidth at this time (there is anticipation of doubling the current data rate), there is no handshaking or sequence numbering identified in this data transfer. Therefore the possibility of data loss without detection exists.

Recommendation 4.13. Investigate the CCMS to Shuttle Data Center and PCGOAL for the possibility of data loss without detection.

Finding 4.14. On pages 90-92, investigate usage of custom protocol instead of test and checkout procedure (TCP) in PCGOAL.

Recommendation 4.14. Explain why there is a need for a custom protocol instead of the industry standard TCP. Explain the level of testing and qualification that is performed for this custom protocol.


Finding 4.15. The review meetings used the terms “reliability” very frequently. However, the study/document does not present a reliability model (i.e., reliability block diagram) from which the predictive models would follow.

Recommendation 4.15. If the intent of the study/analysis is to derive a system reliability, then develop a Reliability Block Diagram (RBD) of the network system to include all hardware elements and corresponding redundancies, if used, in addition to the existing data reliability blocks. Use this RBD as the basis for formulating the mathematical model(s) to derive the system reliability. Hardware reliability does/will have an impact on data reliability. In deriving this formulation, it would be very useful to explicitly state the success (or failure) criteria being used to assess system success (or failure).

Finding 4.16. A number of parameters are based on engineering judgment. Examples are p .109, 8.2.4, “3. Percentages based on engineering judgment” and p .109, 8.2.4.1 Memory Errors, “2. Errors per year are based on engineering judgments.” These “engineering judgments” bring into question the validity of the study.

Recommendation 4.16. The results would be more credible if actual in-service data was used to derive the percentage factors or data derived from qualified or peer-reviewed engineering studies, reports or publications applied in the model.

Finding 4.17. Page 111, 8.2.4.2 Disk Errors, “1. k. MTBF: 1,000,000 hours.” A stated MTBF of exactly 1,000,000 hours seems unlikely – brings into question the accuracy of the results. p .113, “Custom Logic ... 50000 = Custom HW MTBF in Hours.” A stated MTBF of exactly 50000 hours seems unlikely – brings into question the accuracy of the results. p .116, “Logic

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 26 of 40

Data Transfers ... 100000 = Custom HW MTBF in Hours.” A stated MTBF of exactly 100000 hours seems unlikely – brings into question the accuracy of the results, same comment p .117.

Recommendation 4.17. Either use in-service data to compute SDC drive MTBF or obtain detailed life test and/or field data from drive manufacturer(s) to derive MTBF to be used in the model. Note: The above recommendations (#4, 6, 7, 8) are based on findings on p. 192 (9.2 Data Integrity Sensitivity) that show that MTBF “Improvement” affect end-to-end undetected failures (the ones of greatest concern) by up to 18%.

Finding 4.18. Page.111, 8.2.4.4 Element Ground Ruled Out. These elements are “ground ruled” out without adequate explanation as to why. Data to substantiate these not being considered, if available, should be made available.

Recommendation 4.18. Derive/cite data or rationale for these items being “zeroed” out.


Finding 4.19 -- The report is heavy on analysis and assumptions and short on data to be put into the model(s). Section 7, Collected Data, is only two pages of 198 in the report. The Team would have expected to see much more measured data regarding existing network performance that would be input to the model(s).

Recommendation 4.19. Gather, analyze and use exiting network performance data to benchmark system performance over time.

Finding 4.20. Page 195, 10.1 CONCLUSION, “By this rationale, COTS network equipment ... does not warrant being added to the Critical Items List.” This is a “leap of faith” encompassing more than just the analysis included in the report. Likely, it is not prudent to posit this recommendation without further assessment(s) of the now-nonexistent requirements for network operations.

Recommendation 4.20. A stated requirement for network operations needs to be defined. Only then can one ascertain whether or not the study would support removing COTS hardware from the CIL. The Team would expect that the position for removing COTS from the CIL would be reinforced if in-service data for COTS equipments can be gathered and analyzed to demonstrate its historical performance; that is, track the operating performance of the various COTS equipment(s) to show its demonstrated reliability/availability. This should be a routinely reported metric. Also, track the reliability/availability of the entire network could be tracked as a routine metric, and follow the trending carefully to determine whether the system is performing statically, getting better, or worse.

Finding 4.21. Rouge Packet - On page 104 of the report in section 7.3 a CORBA packet occurred on the network when it should not have.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 27 of 40

Recommendation 4.21. This did not appear to affect data integrity, but is an indicator of a logical network design issue and should be resolved or understood.

Finding 4.22. Logic Errors - On pages 108 and 109 (Section 8.2.4), logic errors are discussed. The Team does not understand the basis for logic errors. It appeared that it was tied to power supply MTBF.


Recommendation 4.22. If this is so, the Team believes that a subsystem failure (i.e., power supply) should be considered as part of the reliability calculation rather than data integrity analysis. The Team believes the analysis in this report generally assumes all hardware is operational.

Finding 4.23. Data Quality Checks - The analysis in this report assumes a variety of error detection/correction mechanisms via both hardware and software. What this system does not seem to contain is meta-data checking. What is meant by this is a check to determine if the final end data product is meaningful. This can be as simple as software limit checks.

Recommendation 4.23. The Team assumes this is probably being done somewhere in the system, but it was not apparent and needs to be clarified. This will also help with the “data impersonation” issue discussed in the report.

Finding 4.24. Model Validity- In a large model such as the one used here for data integrity analysis it is always reassuring to have quantitative evidence to validate the model. The model draws on a variety of sources including engineering judgment, simulated results, and industry data. The model essentially determines the likelihood of undetected errors getting into a final data set. The fact that the errors are undetected by definition makes them impossible to measure and raises questions as to how to validate the model.

Recommendation 4.24. One way to validate the model is to measure detected errors and see if they agree with the model’s prediction, and this should be pursued. This will at least allow verification of the system and subsystem error rates to detect any gross errors in the model’s estimates.


	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 28 of 40

6.0 Recommendation

It is recommended that this report be presented to the Project and request originator as the NESC position on the KSC PCGOAL Data Integrity issue.

7.0 Minority Report (dissenting opinions)

No dissenting opinions were identified within the NESC.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 29 of 40

8.0 Lessons Learned

The following lessons learned address both the general nature of this evaluation and its application to a wider range of NASA programs.

8.1 Customer Expectations


NESC involvement was initiated by KSC Safety and Mission Assurance who elevated this problem for NESC attention due to its complexity and the potential impact to the design and operational employment of critical command and control systems. KSC S&MA requested an independent NESC technical assessment of the methodology employed to assess and retire the PCGOAL data corruption CILs, which resulted from the SAA on Data Impersonation/Corruption. The Program had requested a quantitative look at undetected errors and the risk of data corruption by network equipment. The KSC engineering community developed a method for assessing these data corruption CILs to determine the probability of failure. The results of this assessment may be used to eliminate the CILs entirely by classifying the failures as "not credible." Resolution of this issue has potential to impact numerous SAAs, not only for this system but all others classified "critical" since the methodology used to eliminate these data corruption CILs can be employed elsewhere. It was noted that some small possibility of undetected error can always exist in these systems. To classify these as "not credible" is not possible unless clear metrics and reliability/availability criteria are defined and agreed to.

8.2 Terminology

The Team found that interpretation of the report was at times difficult as a result of lack of acronym definition. Additional description of background information and definition of acronyms would be helpful for future reviews of this type and should be requested by the NESC as a part of the inbrief process.

8.3 Requirements


Quantitative requirements for the system were not provided, and indeed may not be available. It was evident that there is an apparent lack of an overall system performance and reliability requirements; however, performance is continually monitored, although minimal details were provided. Without requirements it is impossible to evaluate the performance and reliability of the system and to determine the fitness of replacement COTS components for the high reliability

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 30 of 40

requirements of the system. The Team was presented with the performance numbers that the system is capable of, and no basis for judging if this was good enough or not good enough.


8.4 Programmatic Processes

A major issue is the large number (over 400) of CILs that are open on the integrity and performance of various components of the end-to-end data system. It was stated during the review that due to time constraints and lack of sufficient staffing, closing all the 400 CILs individually was not possible. There was a lengthy discussion on the validity of the CIL process for this application since most of the components were COTS and, unless each equipment component was replaced with a "better version," nothing could be done to address the CIL. Also, the Team noted that component-level performance does not guarantee overall system performance. The need for and scope of CILs is subject to Program requirements. The Team is not sufficiently familiar with Program requirements to judge the need for multiple as opposed to combined CILs, although the Team did comment on the validity of higher level network provisions such as error detection and correction and standard packet transmission protocols as appropriate and generally accepted mitigations for transmission errors. The overall methodology of the study is a valid engineering approach, subject to the specific recommendations of the Team. However, programmatic requirements may require further discussion and possibly some modification to provide for acceptability of the proposed approach. That determination was beyond the scope of this technical assessment.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 31 of 40


9.0 References

1. Engineering Study HMF HIM Card to Consumer Data Integrity Analysis.
2. KSC-5200-6561 Draft 10.0, Jeffrey D. Lee, March 29, 2004.
3. Engineering Study HMF Sensor to Consumer Data Integrity Analysis KSC-5200-6561 Industries References Draft 7.0, Jeffrey D. Lee, February 13, 2004.
4. A Management Overview of the Findings From Engineer Study HMF HIMs to Consumer Data Integrity KSC-5200-6561, Jeffrey D. Lee, January 6, 2004.
5. Spreadsheet, HMF Errors, Jeffrey D. Lee, April 6, 2004.
6. KSC PC GOAL Data Integrity ITA/I Request NESC Chief Engineer Review, Tim R. Wilson, April 1, 2004.
7. NESC Review Meeting KSC, Engineer Study HFM HIMs to Consumer Data Integrity KSC-5200-6561, Jeff Lee and Larry Carr, April 12, 2004.

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 32 of 40


10.0 List of Acronyms

BER	Bit Error Rate
CCL	Commit Criteria List
CIL	Critical Item List
CLCS	Checkout Launch and Control System
COTS	Commercial-Off-The-Shelf
FEP	Front Eng Processor
FMECA	Failure Mode Effects and Criticality Analysis
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HIM	Hardware Interface Module
HMF	Hypergolic Maintenance Facility
IT/AI	Independent Test/Analysis Inspection
IV&V	Independent Validation and Verification
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LaRC	Langley Research Center
LCC	Launch Control Center
LPS	Launch Processing System
MCC	Mission Control Center
MTBF	Mean Time Between Failures
NDE	NESC Discipline Expert
NESC	NASA Engineering and Safety Center
NRB	NESC Review Board
ORR	Operations Readiness Review
RBD	Reliability Block Diagram
RTF	Return to Flight
S&MA	Safety and Mission Assurance
SAA	System Assurance Analyses
SDC	Shuttle Data Center
SDLC	System Development Life Cycle
SPRT	Super Problem Resolution Team
TCP	Test and Checkout Procedure
USA	United Space Alliance

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 33 of 40

Appendices

- A. Findings and Recommendations Prioritization Metrics Approach
- B. Prioritization Worksheet


	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 34 of 39

Plan Approval and Document Revision History

Approved:	Original signature on file	7/13/04
	NESC Director	Date

Approved	Original signed on file	6/26/06
	NESC Director	Date

Version	Description of Revision	Authors	Effective Date
0.01	Draft	Robert A. Kichak Steven S. Scott	05-10-04
2.0	Edited for Content and Formatting	Robert A. Kichak Steven S. Scott	06-16-05

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 35 of 40


Signature Page

NESC Independent Technical Evaluation Team

Original signature on file
Robert A. Kichak, Co-Lead
NESC Discipline Expert, Power & Avionics

Original signature on file
Steven S. Scott, Co-Lead
NESC Discipline Expert, Software

Original signature on file
Tim R. Wilson
NESC Chief Engineer
NASA Kennedy Space Center

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 36 of 40


Appendix A. Findings and Recommendations Prioritization Metrics Approach

A.1 Criticality of Implementation

Criticality of implementation is a severity indicator that describes the overall level of importance of executing action to implement the recommended changes to mitigate findings. For each finding/recommendation pair, the criticality of implementation was determined by anticipating the impact should the change action not be executed. The Criticality of Implementation Levels were established as an ordinal values based on best practice metrics, thorough review of related documents, and stated objectives. The Criticality of Implementation Levels and associated values are displayed below.

Criticality of Implementation

Criticality of Implementation	Thresholds	Value
Critical	Failure to take action to implement recommended changes <ul style="list-style-type: none"> May result in the study's data integrity methodology being determined as inconclusive, ambiguous and/or ineffective and therefore potentially impact the study's objectives in a manner that may result in perception of loss of assurance, or The nature of the finding and subsequent recommended changes are necessary for the study to be compliant with Federal government regulations 	4
Important	The nature of the finding and subsequent recommended changes are necessary for the study to <ul style="list-style-type: none"> Observe industry best practices or NASA guidance or clarify a technical process or condition that impacts the integrity of the study's conclusions 	3
Low	<ul style="list-style-type: none"> The nature of the finding and subsequent recommended changes are necessary to clarify the study's objectives or other stated conclusions or provide background information or Improve the quality of the readability and organizational structure of the study 	2
Negligible	It is not anticipated that the finding/recommendation has a direct impact to the study and/or NASA objective(s).	1

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 37 of 40

A.2 Viability to Implement


The potential, or viability, to implement a recommended change is dependent on various factors: allocation of fiscal and personnel resources required to execute the change, extent to which the change will impact and affect the technical merits and conclusion of the study, and also the degree to which the NASA's technical infrastructure could be impacted by the change. The table below describes the viability to implement degrees and respective requirements for each level.

Viability to Implement

Degree of Viability	Description	Value
Highly Viable	<ul style="list-style-type: none"> Fiscal and staffing resources are allocated, and Policy exists to support and enable the change, and Technical infrastructure exists and can support implementation activities. 	3
Potentially Viable	<ul style="list-style-type: none"> Fiscal and staffing resources are not allocated, but The existing infrastructure can support implementation activities and Policy either exists or can be easily created. 	2
Not Viable	<ul style="list-style-type: none"> Fiscal and staffing resources are not allocated, and Policy does not exist, and Infrastructure cannot support mitigation activities. 	1

A.3 Level of Effort versus Benefits

Hypothetically, it would be possible to perform all recommended changes if the amount of time, activities required to perform the change, impact to content of the study, and potential for inadvertent impacts to the study's technical merit did not need to be considered. Since this is typically not the case, the feasibility of implementing recommended changes needs to be considered. The table below describes the Level of Effort versus Benefits indicators based on an assessment of the findings and activities associated with performing recommended changes.


	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 38 of 40

Level of Effort versus Benefits

Level of Effort versus Benefits Indicator	Description	Value
Supports	<ul style="list-style-type: none"> • Minimum Effort / Maximum Benefit • Minimum Effort / Moderate Benefit • Activities required to implement recommended changes can be performed without resulting in the need to increase or modify capital expenditures, and • The amount of time to perform the recommended changes is determinable and acceptable by NASA and • It is not expected that the changes or activities associated with implementing the changes will impact the technical merits of the study. 	3
Conditionally Supports	<ul style="list-style-type: none"> • Moderate Effort / Medium to High Benefit • High Effort / High Benefit • Activities required to implement recommended changes can be performed without resulting in the need to increase or modify capital expenditures, or • The amount of time to perform the recommended changes is determinable and acceptable by NASA, or • It is not expected that the changes or activities associated with implementing the changes will impact the technical merits of the study. 	2
Does not Support	<ul style="list-style-type: none"> • High Effort / Potentially Low Benefit • Activities required to perform changes to the study cannot be executed without requiring additional capital expenditures, or • The amount of time required to perform the change(s) is not determinable or acceptable to NASA, or • It is expected that the change itself or activities required to perform the change will result in the presence of technical risk, non-compliance with NASA initiatives, objectives, or Federal regulations. 	1

A.4 Implementation Indicator

An Implementation Indicator (II) is a 3-variable function established by aggregating ordinal values associated with the measurable “factors” of Criticality of Implementation (CI), Viability to Implement (VI), and Level of Effort versus Benefits (LB) to prioritize the recommended changes associated with the Findings. The ordinals for each factor are percentage-weighted to compensate for disparities between factors. Accordingly, Criticality of Implementation is weighted the heaviest at 50% to account for the potential impacts to the study of executing

	NASA Engineering and Safety Center Consultation Position Paper	Document #: RP-04-09	Version: 2.0
Title: KSC PCGOAL System Data Integrity			Page #: 39 of 40

changes. Viability to Implement and Level of Effort versus Benefits are weighted equally at 25% each for a total weight of 50%. Demonstrated mathematically, $II = (.50)CI + (.25)VI + (.25)LB$.


The Implementation Indicator is an ordinal between 1 and 3.5 directly associated with a recommended timeframe in which to perform recommended changes to the study. The ordinal values associated with the “most favorable” II factors are rated from low to high. Therefore, a lower II value represents lower priority than higher II values.

A.5 Recommended Implementation Priority

Implementation of changes has been prioritized according to their respective implementation indicators. The table below shows the implementation priority scenarios based upon the calculated implementation indicator value. The worksheet used to perform the actual assessment is contained in the Appendix B of this report.

Recommended Priority of Implementation

Implementation Indicator (II) Value	Priority of Implementation	Threshold Determination
=3.5, ≥2.6	Recommend change be implemented prior to study acceptance	Changes should be made before the study is formally accepted
<2.6, ≥2.0	Recommend change be implemented after study acceptance	Changes may be made after the study is final but should be eventually be incorporated
<2.0, ≥1.1	Requires further analysis to determine whether change activity is appropriate	Changes require additional evaluation to determine applicability and overall impact to the study
1.0	No Change Recommended	No Action Required

	NASA Engineering and Safety Center Consultation Position Paper		Document #: RP-04-09	Version: 2.0
	Title: KSC PCGOAL System Data Integrity			Page #: 40 of 40

Appendix B. Prioritization Worksheet

Finding	Criticality of Implementation Indicator	Criticality Value	Viability to Implement Indicator	Viability to Implement Value	Levels of Effort versus Benefits Indicator	Level of Effort versus Benefits Indicator	Implementation Indicator	Priority
Findings and Recommendations regarding the CIL Process and Lack of Requirements								
2.1	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.2	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.3	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.4	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.5	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.6	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.7	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
2.8	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
Other Findings and Recommendations								
3.1	Critical	4	Potentially Viable	2	Does not Support	1	2.8	Recommend change be implemented prior to study acceptance
3.2	Critical	4	Potentially Viable	2	Does not Support	1	2.8	Recommend change be implemented prior to study acceptance
3.3	Important	3	Not Viable	1	Does not Support	1	2.0	Recommend change to be implemented after study acceptance
3.4	Negligible	1	Potentially Viable	2	Does not Support	1	1.3	Requires further analysis to determine whether change activity is appropriate
3.5	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
3.6	Negligible	1	Not Viable	1	Does not Support	1	1.0	No Change Recommended
3.7	Critical	4	Potentially Viable	2	Does not Support	1	2.8	Recommend change be implemented prior to study acceptance
3.8	Critical	4	Not Viable	1	Does not Support	1	2.5	Recommend change be implemented after study acceptance
3.9a	Critical	4	Potentially Viable	2	Does not Support	1	2.8	Recommend change be implemented prior to study acceptance
3.9b		#N/A		#N/A		#N/A	#N/A	#N/A
3.9c		#N/A		#N/A		#N/A	#N/A	#N/A
3.9d		#N/A		#N/A		#N/A	#N/A	#N/A
3.10	Low	2	Potentially Viable	2	Conditionally Supports	2	2.0	Requires further analysis to determine whether change activity is appropriate
Specific Recommended Improvements for the Data Integrity Analysis and Report								
4.1	Important	3	Highly Viable	3	Supports	3	3.0	Recommend change be implemented prior to study acceptance
4.2	Important	3	Highly Viable	3	Supports	3	3.0	Recommend change be implemented prior to study acceptance
4.3	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.4	Important	3	Potentially Viable	2	Does not Support	1	2.3	Recommend change be implemented after study acceptance
4.5	Important	3	Potentially Viable	2	Does not Support	1	2.3	Recommend change be implemented after study acceptance
4.6	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.7	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.8	Low	2	Potentially Viable	2	Conditionally Supports	2	2.0	Recommend change be implemented after study acceptance
4.9	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.10	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.11	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.12	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.13	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.14	Important	3	Not Viable	1	Does not Support	1	2.0	Recommend change be implemented after study acceptance
4.15	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.16	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.17	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.18	Critical	4	Not Viable	1	Does not Support	1	2.5	Recommend change be implemented after study acceptance
4.19	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.20	Important	3	Highly Viable	3	Conditionally Supports	2	2.8	Recommend change be implemented prior to study acceptance
4.21	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.22	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance
4.23	Important	3	Potentially Viable	2	Conditionally Supports	2	2.5	Recommend change be implemented after study acceptance
4.24	Critical	4	Potentially Viable	2	Conditionally Supports	2	3.0	Recommend change be implemented prior to study acceptance

Levels of Effort versus					
Criticality	Value	Viability	VM Value	Benefits	LB Value
Negligible	1	Not Viable	1	Does not Support	1
Low	2	Potentially Viable	2	Conditionally Supports	2
Important	3	Highly Viable	3	Supports	3
Critical	4				